## CLAIMS

What is claimed is:

1. A method of monitoring and verifying software on a data processing device, comprising:
   an auxiliary system monitoring the software during runtime on the computer, the auxiliary system existing independently of the computer's processor and memory;
   the auxiliary system searching for a compromise to the software; and
   the auxiliary system restricting access to the computer if the compromise is identified.

2. The method according to Claim 1 wherein the software during runtime is loaded into the computer's memory.

3. The method according to Claim 1 wherein searching for the compromise to the software further comprises examining portions of the computer's memory.

4. The method according to Claim 1 wherein searching for the compromise to the software further comprises copying portions of the computer's memory into a memory on the auxiliary system to identify any compromises to the software.

5. The method according to Claim 1 wherein restricting access to the computer further comprises:
   the auxiliary system alerting a remote system of the compromise; and
   the remote system restricting access to the computer if the compromise is identified.

6. The method according to Claim 1 further comprising a remote system providing the auxiliary system with information pertaining to the software.

7. The method according to Claim 6 wherein providing the auxiliary system with information pertaining to the software further comprises providing the auxiliary system with baseline data for the software.

8. The method according to Claim 1 wherein the auxiliary system comprises a device having direct memory access ("DMA access") to the computer's memory.

9. The method according to Claim 1 wherein the auxiliary system includes an intelligent network interface controller.

10. The method according to Claim 1 wherein monitoring the software further comprises monitoring configuration data for the software.

11. The method according to Claim 10 wherein the configuration data for the software is loaded during runtime into the computer's memory.

12. An article comprising a machine-accessible medium having stored thereon instructions that, when executed by a machine, cause the machine to monitor and verify software on a computer by:
monitoring the software during runtime on the computer independently of the computer's processor and memory;
searching for a compromise to the software; and
restricting access to the computer if the compromise is identified.

13. The article according to Claim 12 wherein the software during runtime is loaded into the computer's memory.

14. The article according to Claim 12 wherein the instructions, when executed by the machine, further cause the machine to monitor and verify the software by examining portions of the computer's memory.

15. The article according to Claim 12 wherein the instructions, when executed by the machine, further cause the machine to monitor and verify the software by copying portions of the computer's memory into the machine-accessible medium.

16. The article according to Claim 12 wherein the instructions, when executed by the machine, further cause the machine to monitor and verify the software by:
alerting a remote system of the compromise; and
the remote system restricting access to the computer if the compromise is identified.

17. The article according to Claim 12 wherein the instructions, when executed by the machine, further cause the machine to monitor and verify the software by a remote system providing information pertaining to the software.

18. The article according to Claim 17 wherein the instructions, when executed by the machine, further cause the machine to monitor and verify the software by the remote system providing baseline data for the software.

19. The article according to Claim 12 wherein the instructions, when executed by the machine, further cause the machine to monitor and verify the software by monitoring configuration data for the software.

20. The article according to Claim 19 wherein the configuration data for the software is loaded during runtime into the computer's memory.

21. An auxiliary processing system, comprising:
a processor;
a memory coupled to the processor; and
a monitoring module capable of accessing the processor and the memory, the monitoring module further capable of monitoring and verifying software during runtime on a computer system.

22. The auxiliary processing system according to Claim 21 wherein the processor, the memory and the monitoring module are isolated from the computer system.

23. The auxiliary processing system according to Claim 22 wherein the processor, memory and monitoring module reside within a virtual machine on the computer system.

24. The auxiliary processing system according to Claim 22 wherein the processor, memory and monitoring module reside on a separate device from the computer system.

25. The auxiliary processing system according to Claim 21 wherein the auxiliary system is capable of being coupled to a remote system.

26. The auxiliary processing system according to Claim 25 wherein the remote system is capable of providing the auxiliary processing system with information pertaining to the software on the computer system.

27. The auxiliary processing system according to Claim 26 wherein the remote system is further capable of providing the auxiliary processing system with baseline data for the software on the computer system.

28. The auxiliary processing system according to Claim 26 wherein the remote system is further capable of providing the auxiliary processing system with configuration data for the software on the computer system.